IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF
GEORGIA
ATLANTA DIVISION

BANK OF RIPLEY, on behalf of itself and all others similarly situated, Plaintiff, v. EQUIFAX INC. Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Bank of Ripley ("Plaintiff") by its undersigned counsel, upon personal knowledge as to itself and its own acts, and upon information and belief as to all other matters, brings this putative class action against Equifax Inc. ("Equifax" or "Defendant"), and alleges as follows:

INTRODUCTION

1. The action arises from the data breach experienced by Equifax between May 2017 and July 2017 ("Equifax Breach"). Unprecedented in scope and impact, the Equifax Breach resulted in the theft of critically-sensitive personal and financial data of at least 143 million Americans. Beyond the risk of identity theft and related fraud that such a breach poses to individuals, such compromised data also poses substantial risks to the financial institutions who must bear the financial

brunt of fraudulent charges arising from identity theft and who separately rely on personal and financial consumer data for their lending activity.

2. Plaintiff brings this class action on behalf of financial institutions that suffered, and continue to suffer, financial losses and increased data security risks that are a direct result of Equifax's egregious failure to safeguard the highly-sensitive, personally-identifiable-information in its care, including, but not limited to individuals' (1) personally-identifiable information ("PII"), including but not limited to names, Social Security numbers, birth dates, addresses, and driver's license numbers and (2) payment card data ("Payment Card Data"), including but not limited to credit and debit card numbers, primary account numbers ("PANs"), card verification value numbers ("CVVs"), expiration dates and zip codes. The Equifax Breach has affected over 143 million U.S. banking customers, and has caused direct harm to Plaintiff and the class it seeks to represent. Equifax's actions left highly sensitive PII and Payment Card Data exposed and accessible to hackers for months. Consequently, Plaintiff has incurred and will continue to incur significant damages in cancelling and replacing customers' payment cards, covering fraudulent purchases, taking protective measures to reduce risk of identity theft and loan fraud, and assuming financial responsibility for various types of fraudulent activity related to stolen identities and misuse of PII and Payment Card Data, among other things.

3. Between May 2017 and July 2017, Equifax was subject to one of the

largest data breaches in this country's history when intruders gained access to the highly sensitive PII of over 143 million U.S. consumers—roughly 44% of the United States population—as well as the Payment Card Data for an untold number of credit and debit cards. Despite the fact that the threat of a data breach has been a well-known risk to Equifax, as it acknowledged in its corporate filings, Equifax failed to take reasonable steps to adequately protect the only product in which it exclusively trades and is responsible for protecting: the personal and financial information of millions of individuals. Plaintiff and the class are now left with the direct consequences of Equifax's failures.

4. The data breach was the inevitable result of Equifax's longstanding approach to the security of consumers' confidential data, an approach characterized by neglect, incompetence, and an overarching desire to minimize costs.

5. Equifax's data security deficiencies were so significant that, even after hackers entered its systems, their activities went undetected for at least two months, despite red flags that should have caused Equifax to discover their presence and thwart, or at least minimize, the damage.

6. The financial harms caused by Equifax's negligent handling of PII and Payment Card Data have been, and will be, borne in large part by the financial institutions that issue payment cards, process and hold various loans and credit

products, and service accounts that have been compromised by the breach. These costs include, but are not limited to, canceling and reissuing an untold number of compromised credit and debit cards, reimbursing customers for fraudulent charges, increasing fraudulent activity monitoring, taking appropriate action to mitigate the risk of identity theft and fraudulent loans, sustaining reputational harm, and notifying customers of potential fraudulent activity.

7. Plaintiff seeks to recover the costs that it and others similarly situated have been forced to bear as a direct result of the Equifax data breach and to obtain appropriate equitable relief.

PARTIES

8. Plaintiff Bank of Ripley is a is a locally-owned community bank headquartered in Ripley, Tennessee. It provides banking services for individual and business customers throughout the State of Tennessee. Plaintiff's customers had their PII and/or Payment Card Data stolen as a result of the Equifax Breach.

9. Defendant Equifax Inc. is a publicly traded corporation with its principal place of business at 1550 Peachtree Street NE, Atlanta, Georgia.

JURISDICTION AND VENUE

10. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d). The aggregated claims of the individual class members exceed the sum or value of $5,000,000 exclusive of

interest and costs; there are more than 100 putative class members defined below; and minimal diversity exists because the majority of putative class members are citizens of a different state than Defendant.

11. This Court has personal jurisdiction over Defendant because it maintains its principal headquarters in Georgia, is registered to conduct business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant intentionally avails itself of this jurisdiction by conducting its corporate operations here and promoting, selling, and marketing Equifax products and services to resident Georgia consumers and entities.

12. Venue is proper in this District under 28 U.S.C. §1391(a) because Equifax's principal place of business is in Georgia, and a substantial part of the events, acts, and omissions giving rise to the claims of the Plaintiff occurred in this District.

FACTUAL ALLEGATIONS

13. Equifax is one of the largest and oldest consumer credit reporting agencies in the United States. Equifax has over $3 billion in annual revenue, and its common stock is traded on the New York Stock Exchange.

14. Equifax gathers and maintains credit-reporting information on over 820 million individual consumers and over 91 million businesses.

15. For consumer files, Equifax collects a substantial amount of sensitive

personal information. Equifax's consumer credit files include individuals' PII such as names, current and past addresses, birth dates, social security numbers, and telephone numbers; credit account information, including the institution name, type of account, date the account was opened, payment history, credit limit, and balance; credit inquiry information, including credit applications; and public-record information, including liens, judgments, and bankruptcy filings.

16. Equifax analyzes the information that it collects and generates consumer credit reports, which it sells to businesses like retailers, insurance companies, utility companies, banks and financial institutions, and government agencies.[1]

17. Equifax also provides services to consumers, including credit monitoring and identity-theft-protection products. Additionally, Equifax is required by law to provide one free annual credit report to consumers.

18. Equifax has an obligation to consumers to use every reasonable measure to protect the sensitive consumer information that it collects from exposure to hackers and identity thieves.

The Equifax Breach

19. From mid-May to late July of 2017, hackers exploited a vulnerability

[1] Equifax, *Cybersecurity Incident & Important Consumer Information* (Sept. 8, 2017), https://www.equifaxsecurity2017.com/.

in Equifax's U.S. web server software to illegally gain access to certain consumer files. Investigators believe that the point of entry may have been an open-source software application called Apache Struts, which Equifax used in the customer-dispute portal for its website.[2]

20. The potential vulnerability of the Apache Strut software was no secret. Security researchers with Cisco Systems Inc. warned in March 2017 that a flaw in the Apache Struts software was being exploited in a "high number" of cyber attacks. Despite this warning, Equifax continued to use the software. Equifax was reportedly using an outdated version of Apache Struts at the time of the data breach.[3]

21. Over this nearly three-month period, the Equifax hackers accessed consumer names, social security numbers, birth dates, addresses, and driver's license numbers. The compromised data contains complete profiles of consumers whose personal information was collected and maintained by Equifax.

22. Equifax estimates that 143 million Americans were impacted by this breach, although it admits that it is still in the process of "conducting a

[2] Anna Maria Androtis *et al.*, *Equifax Hack Leaves Consumers, Financial Firms Scrambling*, WALL STREET JOURNAL, Sept. 8, 2017, *available at* https://www.wsj.com/articles/equifax-hack-leaves-consumers-financial- firms-scrambling-1504906993; *see also* Lily Hay Newman, *Six Fresh Horrors From the Equifax CEO's Congressional Hearing*, WIRED, Oct. 3, 2017, *available at* https://www.wired.com/story/equifax-ceo-congress-testimony/.

[3] *Id.*

comprehensive forensic review" with a cybersecurity firm "to determine the scope of the intrusion."[4]

23. In addition to accessing sensitive personal information, the hackers also accessed an estimated 209,000 consumer credit card numbers, and an estimated 182,000 dispute records containing additional personal information were compromised.[5]

24. Equifax reportedly discovered this breach on July 29, 2017.[6]

25. After Equifax discovered this breach but before Equifax disclosed the breach to the public, three high-level executives sold shares in the company worth nearly $1.8 million.[7] On August 1, just three days after Equifax discovered the breach, Equifax Chief Financial Officer John Gamble sold $946,374 worth of stock, and President of U.S. Information Solutions Joseph Loughran exercised options to sell $584,099 worth of stock. The next day, President of Workforce Solutions, Rodolfo Ploder, sold $250,458 worth of stock.

26. Equifax did not report this breach to the public until September 7,

---

[4] Equifax, *Cybersecurity Incident & Important Consumer Information* (Sept. 8, 2017), https://www.equifaxsecurity2017.com/.

[5] *Id.*

[6] *Id.*

[7] Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, BLOOMBERG (Sept. 7, 2017), *available at* https://www.bloomberg.com/news/articles/2017-09-07/three-equifax- executives-sold-stock-before-revealing-cyber-hack.

2017. Equifax has not explained its delay in reporting this breach to the public.

27. Since the breach was publicly revealed, federal regulators have said that they are examining Equifax's actions. The FBI is also investigating the breach,[8] and Congressional hearings have been held regarding the breach.[9]

28. Upon information and belief, although months have passed since Equifax discovered the breach, the investigation is still ongoing, and the identity of the hackers is still unknown.

29. This breach is one of the largest data breaches in history, due to both the number of people exposed and the sensitivity of the information compromised. As reported by the Wall Street Journal, "[t]he Equifax hack is potentially the most dangerous of all, though, because the attackers were able to gain vast quantities of personal identification— names, addresses, Social Security numbers and dates of birth—at one time."[10]

30. The Equifax Breach is unique because many consumers may not be aware that their personal information was compromised. Equifax obtains its credit reporting information from banks, credit card issuers, retailers, lenders, and public records. Accordingly, many consumers are not aware that Equifax or other

---

[8] Androtis, *supra*.

[9] Lily Hay Newman, *Six Fresh Horrors From the Equifax CEO's Congressional Hearing*, WIRED, Oct. 3, 2017, *available at* https://www.wired.com/story/equifax-ceo-congress-testimony/.

[10] *Id.*

reporting companies are collecting or retaining their sensitive personal information.

Financial Institutions and Their Customers Are Harmed by the Breach

31. Initial reports indicate that hackers accessed credit card information of over 200,000 U.S. consumers in this breach. Identity thieves can use these numbers to make fake credit cards, which can then be sold or used to make unauthorized purchases that are then charged to a member's or customer's account.

32. Additionally, sensitive personal and financial information like the information compromised in this breach is extremely valuable to thieves and hackers. These criminals have gained access to complete profiles of individuals' personal and financial information. They can then use these data sets to steal the identities of the consumers whose information has been compromised or sell it to others who plan to do so. The identity thieves can assume these consumers' identities (or create entirely new identities from scratch) to make transactions or purchases, open credit or bank accounts, apply for loans, forge checks, commit immigration fraud, obtain a driver's license in the member's or customer's name, obtain government benefits, or file a fraudulent tax return.

33. When identity thieves fraudulently use a victim's personal information, the victim frequently suffers financial consequences. A 2014 Department of Justice report on identity theft reported that 65% of identity theft

victims experienced direct or indirect financial losses. In addition to the damage caused to consumers, credit unions and banks ultimately bear significant additional losses, as they typically indemnify their customers or members for fraudulent charges.

34. When sensitive personal information is compromised, consumers must exercise constant vigilance on their financial and personal records to ensure that fraudulent activity has not occurred. Consumers are forced to spend additional time monitoring their credit and finances as well as dealing with any potentially fraudulent activity. In turn, the banks and credit unions where these consumers bank must do the same. Consumers also face significant emotional distress after theft of their identity. The fear of financial harm can cause significant stress and anxiety for many consumers. According to the Department of Justice, an estimated 36% of identity theft victims experienced moderate or severe emotional distress as a result of the crime.[11]

35. This also impacts financial institutions negatively and meaningfully. Financial institutions are forced to expend additional customer service resources helping their concerned customers. Customers experiencing severe anxiety related to identity theft are often hesitant to use some banking services altogether, instead opting to use cash. As a result, financial institutions forgo many of the transaction

[11] *Id.*

fees, ATM fees, interest, or other charges that they may have otherwise collected on these accounts.

36. Financial institutions—both those used by legitimate consumers and those used by identity thieves—also feel the financial impact of identity theft.

37. When credit or debit card information is compromised, financial institutions face significant costs, as issuers of those cards, in cancelling and reissuing those payment cards to members or customers. Cancelling the compromised card numbers and reissuing new credit cards to their members or customers is the only way financial institutions can ensure accounts are not charged for unauthorized purchases. Some consumers even change or close their accounts in the wake of the fraud, resulting in additional cost and lost profits to the financial institution.

38. Moreover, financial institutions like Plaintiff are responsible for any fraudulent activity on their members' accounts. When fraudulent charges are made to members' or customers' existing (legitimate) accounts, financial institutions largely bear the cost of indemnifying these charges. For instance, when a member reports fraudulent activity on a credit or debit card, Plaintiff must credit back to its member the amount of any fraudulent charge. Yet Plaintiff has no recourse to recover the charge against the retailer or merchant where the fraudulent purchase was made.

39. Financial institutions face even larger costs associated with entirely new accounts created by identity thieves. With the complete data sets that hackers have now acquired from the Equifax Breach, criminals can use these stolen identities or create a new identity from scratch. They can then use this identity to apply for new lines of credit, loans, or other accounts with financial institutions.

40. Financial institutions are responsible for *all* charges to these fraudulently opened accounts. The losses associated with these newly opened accounts only increase over time. When complete consumer profiles have been compromised, financial institutions experience continuous losses as identity thieves move on from one consumer profile to the next. With a breach of this magnitude, there is virtually no limit to the amount of fraudulent account openings financial institutions may face.

41. Further, financial institutions have an affirmative duty pursuant to, *inter alia*, the Fair Credit Reporting Act to take steps to identify and mitigate risks related to identity theft. *See, e.g.*, 16 C.F.R. § 681.1, "Duties regarding the detection, prevention, and mitigation of identity theft." Such obligations include, but are not limited to, the establishment and implementation of identity theft prevention programs for consumer accounts. *Id*. While the depth, breadth, and impact of the Equifax Breach has yet to be fully understood, one obvious consequence of the breach is the increased difficulties and obligations placed upon

financial institutions in discharging their obligations under regulations such as 16 C.F.R. § 681.1.

42. These risks are very real in the wake of the Equifax Breach. These financial institutions and their members' or customers' information have been compromised as part of the Equifax Breach.

43. As a result, financial institutions face considerable costs associated with monitoring, preventing, and responding to fraudulent charges and account openings. Financial institutions must implement additional fraud monitoring and protection measures, investigate potentially fraudulent activity, and indemnify members or customers for fraudulent charges. Financial institutions also will need to take other necessary steps to protect themselves and their members or customers, including notifying members or customers, as appropriate, that their accounts may have been compromised. These burdens impact credit unions, who frequently serve individual and small business customers.

44. Financial institutions will also face increased regulatory compliance costs going forward because of this incident. Federal regulators have already begun considering the implications of the breach and are likely to implement additional requirements to protect consumers from the financial risks associated with this breach. For example, additional reports and plans will likely be required to satisfy regulators. Financial institutions will be required to directly bear the

costs of these additional measures.

45. Financial institutions are also concerned about the chilling effect this breach may have on future lending as consumers deal with the impact of the breach on their finances and credit, as well as on their emotional wellbeing. Customers or members are often without access to their accounts for several days at a time while credit or debit cards are replaced or accounts are changed. Additionally, some customers are hesitant to use card transactions altogether in the wake of a major breach. This results in lost fees and interest to the financial institutions issuing these cards.

46. Equifax had a duty to properly secure its website from hackers, to use available technology to encrypt and otherwise secure consumers' personal information using industry standard methods, and to act reasonably to prevent the foreseeable harm to Plaintiff and the Class, which it knew would result from a data breach.

47. Indeed, Equifax's role as a credit-reporting firm made the need for it to secure the information it held especially acute. And that role has itself created an additional burden for financial institutions, who have typically relied on the files at credit-reporting agencies like Equifax to determine whether applications for consumer credit or loans are creditworthy. Not only has that process now been thrown into jeopardy for Plaintiff and the financial institutions it seeks to represent,

but also such financial institutions are now without a vital source of verifying consumers' identities due to the extent of the personal and financial information compromised by the Equifax Breach.[12]

48. For all of these reasons, the breach has sent shockwaves throughout the entire financial services industry, and its reverberations will be felt for years to come.

The Breach was the Result of Equifax's Failure to Properly and Adequately Secure its Website

49. The Equifax Breach was the direct result of Equifax's failure to properly and adequately secure its U.S. website.

50. Specifically, Equifax failed to heed warnings from security experts about the vulnerabilities in its Apache Strut software. Additionally, Equifax failed to update this software to its latest version.

51. Equifax admitted in public statements that hackers were able to access this data by exploiting a vulnerability in Equifax's U.S. website application to illegally gain access to consumer files.

52. Equifax should have recognized and identified the flaws in its data

[12] *See* Telis Demos, *Equifax Hack Could Slow Down Fast Loans*, WALL STREET JOURNAL (Sept. 11, 2017), *available at* https://www.wsj.com/articles/equifax- hack-could-slow-down-fast-loans-1505147969.

security and should have taken measures to fix these vulnerabilities. Equifax had a duty to take advantage of what experts had already learned about security vulnerabilities and to use industry best practices, such as updating software to the latest version, to prevent a security breach.

53. Even before this incident, Equifax was on notice of potential problems with its web security. A security researcher has reported that in August, hackers claimed to have illegally obtained credit-card information from Equifax, which they were attempting to sell in an online database.[13] Equifax had a duty to respond to a report of a significant software security flaw. Despite Equifax's knowledge of these potential security threats, Equifax willfully (or at least negligently) failed to enact appropriate measures to ensure the security of its consumer files, including failing to encrypt sensitive personal and financial consumer information.

54. The harm to financial institutions and to their customers as a result of Equifax's failure to adequately secure its computer systems and websites was therefore foreseeable to Equifax.

55. Equifax is well aware of the costs and risks associated with identity

[13] Androtis, *supra*.; *See also,* Thomas Fox-Brewster, *A Brief History of Equifax Security Fails,* FORBES, Sept. 8, 2017, available at: https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data- breach-history/#63dc4270677c.

theft. On its website, Equifax lists "some of the ways identity theft might happen," including when identity thieves "steal electronic records through a data breach."[14]

56. In fact, Equifax has published a report on the "Emotional Toll of Identity Theft." In its report, Equifax states that "identity theft victims may experience similar emotional effects as victims of violent crimes, ranging from anxiety to emotional volatility." The report also cites a survey finding that "69 percent felt fear for personal financial security; 50 percent of respondents said they had feelings of powerlessness or helplessness; and 29 percent said they felt shame or embarrassment."[15]

57. Financial institutions are on the front lines following a data breach, working with these consumers when identity theft does occur, increasing the cost to financial institutions.

58. Because Equifax is aware of the negative consequences of identity theft, Equifax also offers products aimed at protecting consumers from identity theft. For example, Equifax advertises its "Equifax Complete™ Premier Plan" as "Our Most Comprehensive Credit Monitoring and Identity Protection Product."[16]

---

[14] Equifax, *How Does Identity Theft Happen?*, https://www.equifax.com/personal/education/identity-theft/how-does- identity-theft-happen (last accessed September 10, 2017).

[15] Equifax, *A Lasting Impact: The Emotional Toll of Identity Theft*, Feb. 2015, *available at* https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf.

[16] Equifax, *Equifax Complete ™ Premier Plan: Our Most Comprehensive*

The product promises to alert consumers of changes to their credit score and credit report, to provide text message alerts to changes, lock the consumer's credit file by unapproved third parties, and automatically scan suspicious websites for consumers' personal information.

59. Equifax was aware of the risk posed by its insecure and vulnerable website. It was also aware of the extraordinarily sensitive nature of the personal information that it maintains as well as the resulting impact that a breach would have on financial institutions (and their customers)—including Plaintiff and the other Class members.

Equifax Had a Duty to Prevent and Timely Report this Breach

60. Equifax had a duty to prevent breach of consumers' sensitive personal information.

61. Following several high-profile data breaches in recent years, including Target, Home Depot, Yahoo, and Sony, Equifax was on notice of the very real risk that hackers could exploit vulnerabilities in its data security. Moreover, Equifax has considerable resources to devote to ensuring adequate data security.

62. Nonetheless, Equifax failed to invest in adequate cyber security

Credit Monitoring and Identity Protection Product, https://www.equifax.com/personal/products/credit/monitoring-and-reports (last accessed Sept. 10, 2017).

measures to properly secure its U.S. website from the threat of hackers.

63. Financial institutions and consumers were harmed not only by the breach itself but also by Equifax's failure to timely report this breach to the public.

64. Equifax discovered this breach on July 29, 2017, but did not report it to the public until nearly six weeks later on September 7, 2017.

65. According to the Wall Street Journal, an anonymous source familiar with the investigation states that "Equifax executives decided to hold off on informing the public until they had more clarity on the number of people affected and the types of information that were compromised."[17] But Equifax has not yet given an official explanation for its delay in reporting this breach to the public. In the time between when Equifax discovered this breach and when it reported the breach to the public, however, three of its top executives were able to sell—and sold—substantial sums of stock in the company, presumably avoiding the financial losses associated with the negative press Equifax has received since the breach.[18]

66. Because of this delay, consumers with compromised personal information and credit card information have been unable to adequately protect

[17] Androtis, *supra*.

[18] Equifax's stock prices dropped almost 15% the day after the breach was publicly announced—the largest decline in nearly two decades. Ben Eisen, *Equifax Shares on Pace for Worst Day in 18 Years*, WALL STREET JOURNAL (Sept. 8, 2017), *available at* https://blogs.wsj.com/moneybeat/2017/09/08/equifax- shares-on-pace-for-worst-day-in-18-years/.

themselves from potential identity theft for several weeks.

67. Financial institutions have also been unable to alert their members or customers of the risk in a timely manner, or to implement measures to detect and prevent potential fraud in the time before the breach was disclosed.

68. This resulted in additional harm to Plaintiff, the Class, and consumers that they would not have suffered if Equifax had not delayed in reporting the breach to the public.

69. As a result of the PII and Payment Card Data compromised in the Equifax Breach, Plaintiff has suffered and will continue to suffer direct injury in the form of, *inter alia*, increased burdens associated with regulatory obligations to guard against identify theft (as described above), increased burdens associated with additional due diligence associated with lending, and loss of customer goodwill.

CLASS ALLEGATIONS

70. Plaintiff brings this action on behalf of itself and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of the following class of payment card issuing and lending financial institutions ("the Class"):

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) who issue payment cards and/or otherwise extend credit to consumers.

71. This action may properly be maintained as a class action and satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

72. Numerosity. The members of the class are so numerous that joinder would be impracticable. Plaintiff believes the number of Class members exceeds 10,000.

73. Commonality. There are common questions of law and fact that predominate over questions affecting only individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Equifax owed a duty to Plaintiff and members of the Class to protect PII and Payment Card Data;

b. Whether Equifax failed to provide reasonable security to protect PII and Payment Card Data;

c. Whether Equifax negligently or otherwise improperly allowed PII and Payment Card Data to be accessed by third parties;

d. Whether Equifax failed to adequately notify Plaintiff and members of the Class that its data systems were breached;

e. Whether Plaintiff and members of the Class were injured and

suffered damages and ascertainable losses;

f. Whether Equifax's failure to provide reasonable security proximately caused the injuries suffered by Plaintiff and members of the Class;

g. Whether Plaintiff and members of the Class are entitled to damages and, if so, the measure of such damages; and

h. Whether Plaintiff and members of the Class are entitled to declaratory and injunctive relief.

74. Typicality. Plaintiff's claims are typical of the claims of the absent Class members and have a common origin and basis. Plaintiff and absent Class members are all financial institutions injured by Equifax's data breach. Plaintiff's claims arise from the same practices and course of conduct giving rise to the claims of the absent Class members and are based on the same legal theories, namely Equifax's liability stemming from the data breach. If prosecuted individually, the claims of each Class member would necessarily rely upon the same material facts and legal theories and seek the same relief.

75. Adequacy. Plaintiff will fully and adequately assert and protect the interests of the absent Class members and have retained counsel who are experienced and qualified in prosecuting class action cases similar to this one. Neither Plaintiff nor its attorneys have any interest contrary to or conflicting with

the interests of absent Class members.

76. The questions of law and fact common to all Class members predominate over any questions affecting only individual Class members.

77. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class members' claims is economically infeasible and procedurally impracticable. Class members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class members to litigate their claims where it would otherwise be too expensive or inefficient to do so. Plaintiff knows of no difficulties in managing this action that would preclude its maintenance as a class action.

COUNT I
Negligence

78. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

79. Equifax owed—and continues to owe—a duty to Plaintiff and members of the Class, to use reasonable care in safeguarding PII and Payment Card Data and to notify them of any breach in a timely manner so that appropriate action can be taken to minimize or avoid losses. This duty arises from several

sources, including, but not limited to, the sources described below, and is independent of any duty Equifax owed as a result of any of its contractual obligations.

80. Equifax has a common law duty to prevent the foreseeable risk of harm to others, including Plaintiff and the Class. The duty to protect others against the risk of foreseeable criminal conduct has been recognized in situations in which the parties are in a special relationship, or where an actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk. *See* Restatement (Second) of Torts, §302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard PII, Payment Card Data, and other sensitive information.

81. It was foreseeable that injury would result from Equifax's failure to use reasonable measures to protect PII and Payment Card Data and to provide timely notice of a breach. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal PII and/or Payment Card Data belonging to millions of consumers; thieves would use the PII and Payment Card Data to create the injury and damages described herein.

82. There is no question that the prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the

United States. According to the Identity Theft Resource Center, the year 2016 saw a total of 1,093 reported data breaches in the United States, an all-time high.[19] More than 36 million records were reportedly exposed in those breaches.[20]

83. It is well known that a common motivation of data breach perpetrators is the hackers' intentions to sell PII and/or Payment Card Data on underground black markets, and news outlets reported that this, in fact, occurred after the Home Depot and Target data breaches, among others. Malicious or criminal attacks were the cause of 50% of the breaches covered by the IBM study, and were also the most costly.[21]

84. In tandem with the increase in data breaches, the rate of identity theft also reached record levels in 2016, affecting approximately 15.4 million victims in the United States and resulting in approximately $16 billion worth of fraud losses.[22] In this environment, every reasonable person and company in the United States is aware of the significant risk of criminal attacks against computer systems

---

[19] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html.

[20] *Id.*

[21] *Id.*

[22] Javelin Strategy & Research, *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study* (Feb. 1, 2017), *available at* https://www.javelinstrategy.com/press- release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent- according-new.

that store PII, Payment Card Data and other sensitive information.

85. Equifax assumed the duty to use reasonable security measures as a result of its conduct, internal policies and procedures, and Privacy Policy in which the company stated it was using "industry standard means" of protecting PII and Payment Card Data, and that its security measures were "appropriate for the type of information we collect." By means of these statements, Equifax specifically assumed the duty to comply with industry standards, including PCI DSS and every other conceivable standard applicable to a company whose sole business is transacting in the most sensitive consumer information there is.

86. A duty to use reasonable security measures also arises as a result of the special relationship that existed between Equifax and Plaintiff and the Class. The special relationship arises because financial institutions entrusted Equifax with customer PII and Payment Card Data. Only Equifax was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

87. Equifax's duty to use reasonable data security measures also arises under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by retailers such as Equifax. FTC publications and data

security breach orders further form the basis of Equifax's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

88. Equifax's duty to use reasonable care in protecting PII and Payment Card Data arises not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

89. Equifax Breached its common law, statutory and other duties—and was negligent—by failing to use reasonable measures to protect consumers' personal and financial information from the hackers who perpetrated the data breach and by failing to provide timely notice of the breach. The specific negligent acts and omissions committed by Equifax include, but are not limited to, the following:

a. failure to employ reasonable systems to protect against malware;

b. failure to regularly and reasonably update its antivirus software;

c. failure to maintain an adequate firewall;

d. failure to reasonably track and monitor access to its network and consumer data;

e. failure to reasonably limit access to those with a valid purpose;

f. failure to heed warnings about specific vulnerabilities in its systems identified by Equifax's own employees, consultants, and software vendors;

g. failure to recognize red flags signaling that Equifax's systems were inadequate and that, as a result, the potential for a massive data breach akin to the one involving Target and Home Depot was increasingly likely;

h. failure to recognize that for approximately eight months hackers were stealing PII and Payment Card Data from its systems while the data breach was taking place; and

i. failure to disclose the data breach in a timely manner.

90. As a direct and proximate result of Equifax's negligence, Plaintiff and the Class have suffered and continue to suffer injury as described herein.

91. Because no statutes of other states are implicated, Georgia common law applies to the negligence claims of Plaintiff and the Class.

COUNT II
Negligence Per Se

92. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

93. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted

and enforced by the FTC, the unfair act or practice by consumer-serving organizations such as Equifax of failing to use reasonable measures to protect PII and Payment Card Data. The FTC publications and orders described above also form the basis of Equifax's duty.

94. Equifax violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and Payment Card Data and by not complying with applicable industry standards, including PCI DSS. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach at a major credit reporting agency, including specifically the immense damages that would result to consumers and financial institutions.

95. Equifax's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

96. Plaintiff and the Class are within the scope of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for paying for and reimbursing consumers for fraud losses. Moreover, many of the class members are credit unions, which are organized as cooperatives whose members are consumers.

97. Furthermore, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has

pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class here.

98. As a direct and proximate result of Equifax's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury and damages as described herein.

99. Because no statutes of other states are implicated, Georgia common law applies to the negligence per se claim of Plaintiff and the Class.

COUNT III
Declaratory and Equitable Relief

100. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

101. Under the Declaratory Judgment Act, 28 U.S.C. §2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and that violate the terms of the federal and state statutes described in this complaint.

102. An actual controversy has arisen in the wake of Equifax's data breach regarding its common law and other duties to reasonably safeguard its customers' PII and Payment Card Data. Plaintiff alleges that Equifax's data security measures were inadequate and remain inadequate. Furthermore, Plaintiff continues to suffer

injury and damages as described herein.

103. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Equifax continues to owe a legal duty to secure PII and Payment Card Data under, *inter alia*, the common law and Section 5 of the FTC Act;

b. Equifax continues to breach its legal duty by failing to employ reasonable measures to secure PII and Payment Card Data; and

c. Equifax's ongoing breaches of its legal duty continue to cause Plaintiff harm.

104. The Court should also issue corresponding injunctive relief requiring Equifax to employ adequate security protocols consistent with industry standards to protect PII and Payment Card Data. Specifically, this injunction should, among other things, direct Equifax to:

a. implement encryption keys in accordance with industry standards;

b. consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;

c. audit, test, and train its data security personnel regarding any

new or modified procedures and how to respond to a data breach;

d. regularly test its systems for security vulnerabilities, consistent with industry standards; and

e. install all upgrades recommended by manufacturers of security software and firewalls used by Equifax.

105. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Equifax, which is a real possibility given the continued missteps taken by Equifax described herein, including using its official corporate communications to send affected consumers to phishing sites. Indeed, Equifax was hit with a separate data breach in March 2017 that apparently did nothing to motivate the company to discover the other massive data breach going on at the same time.[23] The risk of another such breach is real, immediate, and substantial. If another breach at Equifax occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and it will be forced to bring multiple lawsuits to rectify the same conduct.

[23] Mark Coppock, *Equifax Confirms It Suffered A Separate Data Breach In March*, DIGITALTRENDS (Oct. 3, 2017), *available at* https://www.digitaltrends.com/computing/equifax-data-breach-affects-143-million-americans/.

106. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Equifax if an injunction is issued. Among other things, if another massive data breach occurs at Equifax, Plaintiff and the Class will likely incur millions of dollars in damages. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security measures is relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

107. Issuance of the requested injunction will serve the public interest by preventing another data breach at Equifax, thus eliminating the injuries that would result to Plaintiff, the Class, and the potentially millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court:

a. Certify the Class and appoint Plaintiff and Plaintiff's counsel to represent the Class;

b. Enter a monetary judgment in favor of Plaintiff and the Class to compensate them for the injuries they have suffered, together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

c. Enter a declaratory judgment as described herein;

d. Grant the injunctive relief requested herein;

e. Award Plaintiff and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and

f. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims so triable.

Respectfully submitted this 27th day of November, 2017.

COMPLEX LAW GROUP, LLC

By: /s/ David M. Cohen
David M. Cohen
Ga. Bar No. 173503
40 Powder Springs Street
Marietta, GA 30064
Telephone: (770) 200-3100
Facsimile: (770) 200-3101
dcohen@complexlaw.com

CARNEY BATES & PULLIAM, PLLC

Allen Carney (to be admitted *pro hac vice*)
Joseph Henry Bates (to be admitted *pro hac vice*)
519 W. 7th Street
Little Rock, AR 72201
Telephone: (501) 312-8500
Facsimile: (501) 312-8505
acarney@cbplaw.com
hbates@cbplaw.com

Attorneys for Plaintiff and the Proposed Class